

CURRICULUM ASSESSMENT

AUTHORY : TSHINGOMBE

CAREER EDUCATION MATERIAL DIDACTIC & SECURITY SAFETY POLICY

Author: Tshingombe Tshitadi

Overview

This work explores the intersection of **career education, didactic materials, and security/safety policy frameworks**. It examines how engineering principles interact with regulatory policies, and how management systems can deliver traceable, auditable information for both academic and professional environments.

Scope

- **Education & Didactics:** Development of academic materials for technical and vocational training.
- **Security & Safety Policy:** Integration of codes of conduct, licensing, and compliance.
- **Engineering vs Policy:** Experimental approaches to balancing technical innovation with regulatory oversight.
- **Company & Regulatory Frameworks:** Application of standards in organizational and industrial contexts.
- **Management Systems:** Information delivery, auditing, and investigation principles.

Key Description

- **Didactic Academic Material:** Structured learning resources aligned with NQF and SAQA standards.
- **Security Policy & Code of Conduct:** Ethical and professional guidelines ensuring safe environments.
- **Licensing & Defense:** Credentialing processes that validate competence and safeguard public trust.
- **Engineering vs Policy Experimentation:** Case studies where technical solutions challenge or adapt to policy.
- **Regulatory Frameworks:** National and international standards (DHET, PSIRA, IEC, SANS).

Principle Investigation & Data Analysis

- **Methodology:** Comparative analysis of engineering practices vs regulatory compliance.

- **Data Sources:** Academic curricula, company policies, regulatory documents, and incident reports.
- **Investigation Principles:** Traceability, accountability, and transparency in both education and security.
- **Analytical Tools:** Logigrammes, organigrammes, Visual Basic automation for credential validation.

Advantages

- Strengthens **career pathways** through audit-ready education materials.
- Enhances **security resilience** with proactive policy enforcement.
- Promotes **trust and compliance** in engineering and company frameworks.
- Provides **scalable management systems** for information delivery and auditing.

Disadvantages

- Potential **conflict between innovation and regulation**.
- **Resource-intensive** implementation of compliance systems.
- Risk of **fragmentation** when multiple regulatory bodies overlap.
- **Complexity** in aligning academic didactics with industry standards.

Bibliographie

- Microsoft Digital Defense Report (latest edition)
- SAQA & DHET regulatory frameworks
- IEC & SANS engineering standards
- Contributor Covenant v2.1 (Code of Conduct)
- Case studies in education technology and security management

Conclusion

This document defends the position that **career education and didactic materials must be inseparably linked to security and safety policies**. By embedding regulatory frameworks into academic and company systems, organizations can achieve **traceable, auditable, and resilient structures**. The balance between engineering experimentation and policy compliance is critical for sustainable growth, ethical governance, and professional trust.

Would you like me to expand this into a **full thesis-style manuscript** (with detailed chapters and references), or keep it as a **concise executive summary** for presentation and policy briefing?

Contents

CURRICULUM ASSESSMENT	1
AUTHORY : TSHINGOMBE	1
CAREER EDUCATION MATERIAL DIDACTIC & SECURITY SAFETY POLICY	2
 Overview	2
 Scope	2
 Key Description	2
Principle Investigation & Data Analysis	2
 Advantages	3
 Disadvantages	3
 Bibliographie	3
 Conclusion	3
Overview & Scope	7
 Preamble & Key Descriptions	8
Technical Components	8
 Standards & Partnerships	8
Governance & Ethics	8
 Security & Reporting	9
 Project Name	9
 Description	9
 Scope & Objectives	9

Features	9
🖼 Visuals	10
🔧 Installation	10
Usage	10
🛡 Code of Conduct	10
Roadmap	10
Contributing	10
👥 Authors & Acknowledgments	11
📄 License	11
📊 Project Status	11
📅 Event Details	11
🎯 Why Join	11
👥 Who Should Attend	11
📌 Agenda	12
📁 Key Takeaway	12
🔍 Current Security Capabilities	12
🚀 Features Available with GitLab Ultimate	13
🔗 Recommended Next Steps	13
📊 Why This Matters	13
📊 Trial Snapshot	14
🔧 What You Can Do During the Trial	14
Recommended Next Steps	14

 Technical Report Title	17
 Author	18
Overview	18
 Scope	18
 Description	18
 Analysis	18
 Inconveniences	18
 Advantages	19
 Disadvantages	19
 Data Analysis	19
 Investigation Method & Research	19
Inventor Contribution	19
Conclusion	20
 Bibliographic References	20
 Operational Standards: GENIAC & GENIE CORP MILITAIRE	20
  Strategic Report: Support for Energy-Efficient Electrical & Industrial Systems in South Union Africa (S.E.E.E.I.S.U.A)	 23
1.  Overview	23
2. Background	24
3.  Issue Statement	24
4.  Scope	24
5.  Description	24

6.  Data Inventory & Analysis	25
7.  Advantages	25
8.  Disadvantages	25
9.  Mission	25
10.  Vision	26
11.  Goal	26
12.  Operational Framework	26
13.  Module: Infrastructure Overhaul	26
14.  Regulation Framework	26
 DESCRIPTION	27
 ANALYSIS	27
 RESEARCH METHOD	27
 REGULATION SECTOR: ENVIRONMENT	28

Overview & Scope

Operation GENIAC is a multidisciplinary initiative integrating:

- **Military Combat Engineering** (Artillery, Tactical Systems)

- **Security & Safety Engineering** (PSIRA Grades A–E, CCTV, Cabling, Control Rooms)
- **Technical Oversight** (Visual Basic automation, auditing, scenario modeling)
- **Community Governance** (Code of Conduct, enforcement protocols)
- **Strategic Partnerships** (Brigade 119, Edutech, Lab GWorkshop, Office Genie Consultant)

Preamble & Key Descriptions

- **Mission:** Engineer a traceable, auditable, and ethical framework for combat and security operations.
- **Core Domains:**
 - Engineering Police & Safety Systems
 - Military-grade Logic & Automation
 - Collision Scenario Investigation
 - Information Delivery & Auditing
 - Annual Management Reporting

Technical Components

Module	Description
Organigram	Role-based hierarchy for GENIAC operations
Logigram	Workflow logic for credential validation, combat readiness, and scenario response
Visual Basic Code	Automation for diploma validation, control room logic, and asset tracking
Collision Scenario Engine	Models impact, response, and investigation protocols
Audit Layer	Tracks delivery, compliance, and system integrity

Standards & Partnerships

- **Engineering Standards:** MIL-STD, SANS, IEC, PSIRA
- **Partners:**
 - **Brigade 119:** Tactical deployment and combat training
 - **Edutech:** Curriculum and credentialing systems
 - **Lab GWorkshop:** Technical prototyping and diagnostics
 - **Office Genie Consultant:** Strategic planning and systems integration

Governance & Ethics

- **Code of Conduct:** Adapted from Contributor Covenant v2.1
- **Positive Behaviors:**
 - Empathy, respect, constructive feedback, accountability
- **Unacceptable Behaviors:**
 - Harassment, trolling, privacy violations
- **Enforcement:**
 - Correction → Warning → Temporary Ban → Permanent Ban
- **Scope:** Applies across all GENIAC spaces and representations

Security & Reporting

- **Security Protocols:** GitHub Safe Harbor Policy
- **Reporting Channels:** opensource-security[[@](mailto:opensource-security@github.com)]github.com
- **Disclosure Guidelines:**
 - Vulnerability type, source paths, reproduction steps, impact analysis

Project Name

Operation GENIAC: Engineering & Education Technologies Framework

Description

A modular, auditable, and standards-aligned system for engineering education, military-grade logic, and security infrastructure. This project integrates Visual Basic automation, credential dashboards, and scenario modeling for technical and vocational excellence.

Scope & Objectives

- **Credentialing & Auditing:** DHET, PSIRA, SAQA, QCTO compliance
- **Combat & Security Engineering:** GENIE artillery, CCTV, control room logic
- **Education Technologies:** Modular curriculum, Edutech integration
- **Community Governance:** Contributor Covenant v2.1 enforcement
- **Deployment:** GitLab CI/CD, Kubernetes, EC2, ECS

Features

- Logigram & Organigram mapping
- Collision scenario investigation engine
- Visual Basic modules for diploma validation
- Credential dashboard with NQF tracking
- Integration with Brigade 119, Edutech, Lab GWorkshop

Visuals

Include screenshots of:

- Credential dashboard
- Logigram flow
- Control room simulation
- Certificate and badge layouts

Installation

```
bash
cd existing_repo
git remote add origin https://gitlab.com/engineering-tshingombe/thesis-honor-
degre-engineering-and-education-technologie.git
git branch -M main
git push -uf origin main
```

Usage

- Run `ElectricalDiplomaValidator` to validate N4–N6 credentials
- Use `CollisionScenarioEngine` to simulate impact diagnostics
- Deploy dashboards via GitLab CI/CD pipelines

Code of Conduct

Follows Contributor Covenant v2.1. Positive behaviors: empathy, respect, accountability
Unacceptable behaviors: harassment, trolling, privacy violations Enforcement: correction →
warning → ban

Roadmap

- Phase 1: Credential dashboard MVP
- Phase 2: Combat scenario engine
- Phase 3: Edutech curriculum integration
- Phase 4: Visual Basic automation suite

Contributing

Open to contributions. Please follow the Code of Conduct and submit merge requests with clear documentation.

Authors & Acknowledgments

- **Tshingombe Fiston Tshitadi** – Systems Architect
- **Brigade 119** – Tactical Engineering Partner
- **Edutech & Lab GWorkshop** – Curriculum and prototyping support

License

MIT License © 2025 Kananga5

Project Status

Active development. MVP modules deployed. CI/CD pipelines operational.

Would you like me to help you generate a **Visual Basic module**, a **logigram diagram**, or a **credential dashboard layout** next?

Event Details

- **Date:** Tuesday, 20 January 2026
- **Time Zones:**
 - 9:00–10:00 AM (GMT) London, Lisbon, Dublin
 - 10:00–11:00 AM (GMT+1) Berlin, Madrid, Paris, Rome, Prague
 - 11:00–12:00 PM (GMT+2) Bucharest, Athens, Helsinki, Cairo, Nairobi
 - 1:00–2:00 PM (GMT+4) Abu Dhabi, Muscat
- **Where:** Online (registration required)
- **Language:** English
- **Closed Captioning:** English, Deutsch, Français

Why Join

- **Explore cyber trends** from the Microsoft Digital Defense Report.
- **See Microsoft Security Services in action**, with proactive solutions for anticipating risks.
- **Learn resilience strategies** from CISOs and industry leaders.
- **Walk away with actionable recommendations** to strengthen defenses and accelerate recovery.

Who Should Attend

- Chief Information Security Officers (CISOs)
- Chief Information Officers (CIOs)

- Security IT Specialists & SOC Analysts
- Security Practitioners
- IT Decision Makers (ITDMs)

✈ Agenda

Time (GMT)	Session	Speaker(s)
09:00–09:10	Event Welcome & Agenda Walkthrough	Tomas Casasco (EMEA Security Go to Market Lead, Microsoft)
09:10–09:30	Cybersecurity Emerging Trends: Insights from Microsoft Digital Defense Report	Simone Pezzoli (EMEA Chief Security Advisor, Microsoft)
09:30–09:50	Microsoft Security Services Overview	Matteo Polita (EMEA Global Black Belt, One Services, Microsoft)
09:50–10:00	Fireside with CISO from Técnicas Reunidas S.A	Fernando Zamorano Timor (CISO, Técnicas Reunidas), Lucas Alados Linares (Senior Security Specialist, Microsoft)
10:00	Event Wrap-up	Tomas Casasco

🔑 Key Takeaway

This briefing is designed to help organizations **move from reactive defense to proactive resilience**, leveraging Microsoft’s security ecosystem to anticipate, withstand, and recover from cyber threats.

Would you like me to prepare a **personalized checklist** for you—covering how to get the most out of this event (e.g., questions to ask, insights to focus on for your engineering/security background)?

🔍 Current Security Capabilities

- **Static Application Security Testing (SAST)** → *Not enabled*
 - Scans your source code for vulnerabilities before deployment.
- **Infrastructure as Code (IaC) Scanning** → *Not enabled*
 - Checks configuration files (Terraform, Kubernetes YAML, etc.) for misconfigurations.
- **Container Scanning** → *Not enabled*
 - Examines Docker images for known vulnerabilities.
- **Pipeline Secret Detection** → *Not enabled*
 - Detects hardcoded secrets in your repo history.
- **Secret Push Protection** → *Enabled by default for public projects*

- Blocks commits containing API keys or tokens.

⚡ Features Available with GitLab Ultimate

- **Advanced SAST:** Deeper vulnerability analysis with extended rules.
- **DAST (Dynamic Application Security Testing):** Simulates external attacks on running apps.
- **Dependency Scanning:** Flags vulnerable libraries in your codebase.
- **Coverage Fuzzing & API Fuzzing:** Finds bugs by stress-testing inputs.
- **License Information Source:** Ensures compliance with open-source licensing.
- **Container Registry Scanning:** Automatically scans images when pushed.

✂ Recommended Next Steps

1. **Enable SAST** on your default branch to start baseline vulnerability detection.
2. **Add Secret Detection** in your CI/CD pipeline to prevent credential leaks.
3. If you're using Docker/Kubernetes, **turn on Container & IaC scanning**.
4. Consider **upgrading to Ultimate** if you need runtime metrics, dependency scanning, or fuzzing.
5. **Run pipelines** after enabling scanners — results only show once valid artifacts are generated.

🏢 Why This Matters

By enabling these tools, you'll move from **reactive fixes** to **proactive security**, aligning with cyber resilience practices like those highlighted in Microsoft's Digital Defense Report. It's essentially building a **continuous security audit layer** into your engineering workflow.

Would you like me to draft a **step-by-step GitLab CI/CD pipeline configuration** (YAML file) that enables SAST and Secret Detection for your project right away?

You said

tshingombe OPGENIAC TBRIGADE GitLab Duo Get the most out of your trial with space for more members During your trial, invite as many members as you like to tshingombe OPGENIAC TBRIGADE to collaborate with you. When your trial ends, you'll have a maximum of 5 members on the Free tier, or you can get more by upgrading to a paid tier. You have successfully started an Ultimate and GitLab Duo Enterprise trial that will expire on January 09, 2026. To give members access to new GitLab Duo Enterprise features, assign them to GitLab Duo Enterprise seats. GitLab Duo Enterprise Monitor, manage, and customize AI-powered features to ensure efficient utilization and alignment. Seat utilization 1 / 100 A user can be assigned a GitLab Duo Enterprise seat only once each billable month. Start date: Dec 10, 2025 End date: Jan 09, 2026 GitLab Duo Enterprise On by default GitLab Duo Core available to all users Enabled Experiment and beta features Not enabled Model Selection

You've successfully activated a **GitLab Ultimate + GitLab Duo Enterprise trial** for your project **tshingombe OPGENIAC TBRIGADE** 🚀. Here's a quick breakdown so you can make the most of it before it expires on **January 9, 2026**:

Trial Snapshot

- **Plan:** GitLab Ultimate + GitLab Duo Enterprise
- **Trial period:** Dec 10, 2025 → Jan 09, 2026
- **Seats available:** 100 (currently 1/100 in use)
- **Seat rules:** Each user can be assigned a Duo Enterprise seat once per billable month.
- **Features enabled by default:**
 - GitLab Duo Core (AI-powered assistance for all users)
 - Enterprise monitoring and customization tools
- **Not enabled yet:** Experiment & beta features, model selection

What You Can Do During the Trial

- **Invite unlimited members** to collaborate (after trial, Free tier allows max 5 unless upgraded).
- **Assign Duo Enterprise seats** to team members who need advanced AI features (e.g., code suggestions, vulnerability analysis, project insights).
- **Enable security scans** (SAST, Secret Detection, Dependency Scanning, DAST, Fuzzing) since Ultimate unlocks the full suite.
- **Experiment with CI/CD pipelines** for automated testing, deployment, and security auditing.
- **Monitor seat utilization** to ensure the right people have access to Enterprise features.

Recommended Next Steps

- Assign seats to your **core engineering/security team** so they can test Duo Enterprise features.
- Enable **SAST + Secret Detection** in your pipelines to start proactive vulnerability management.
- Explore **AI-powered merge request reviews** and **repository analytics** to see how Duo enhances collaboration.
- Document your workflows during the trial—this helps justify whether to upgrade after January 9.

Technical Report Title

**Support for Energy-Efficient Electrical & Industrial Systems in South Union Africa
(S.E.E.E.I.S.U.A)**

Author

Tshingombe Tshitadi Fiston National-grade curriculum architect, technical educator, and compliance strategist

Overview

This report proposes a unified regulatory and operational framework to support energy-efficient electrical and industrial systems across South Union Africa. It integrates civilian infrastructure, industrial metering, and military-grade standards under a peace-driven, intergovernmental initiative.

Scope

- Interregional energy regulation and dispatching
- City power governance and conflict resolution
- Industrial metering, load shedding, and compliance
- Integration of MIL-STD protocols for strategic infrastructure
- Talent development and job regulation across municipalities

Description

The S.E.E.E.I.S.U.A framework includes:

- Metering systems for single-phase and three-phase installations
- Calibration protocols for kWh, kVA, kVAR, $\cos \phi$, and phase angle
- Substation demolition and remanufacture logic
- Regulation of industrial supply chains, tendered jobs, and energy recycling
- Military-standard (MIL-STD) compliance for strategic installations

Analysis

- **Energy Indexing:** Daily (10 kWh), Monthly (300 kWh/cell), Annual (3600 kWh)
- **Conflict Zones:** Metering discrepancies between consumer and substation
- **Financial Forecast:** 50,000 MW / R50 billion budget
- **Efficiency Metrics:** $\text{Efficiency} = \frac{\text{Output Power}}{\text{Input Power}} \times 100$
 $\text{Loss} = \text{Input Power} - \text{Output Power}$

Inconveniences

- Infrastructure fragmentation
- Regulatory overlap between city and national bodies
- Lack of unified metering standards
- Resistance to remanufacture and modernization

✓ Advantages

- Harmonized energy governance
- Reduced consumer-supplier conflict
- Enhanced audit and compliance tracking
- Integration of military-grade reliability and security

✗ Disadvantages

- High initial cost
- Complex intergovernmental coordination
- Risk of politicization in commissioner roles
- Technical retraining requirements

📊 Data Analysis

Metric	Value
Daily kWh/cell	10
Monthly kWh/cell	300
Annual Index	3600 kWh
Conflict Load	70,000 MW
Budget Forecast	R50 billion

🔍 Investigation Method & Research

- Field audits of city power stations and substations
- Comparative metering between normal and emergency boards
- Simulation of load shedding and transformer efficiency
- Military-grade reliability testing (GENIAC, GENIE CORP protocols)
- Regulatory mapping across municipal and national levels

Inventor Contribution

Tshingombe Tshitadi Fiston

- Architected modular calibration systems
- Designed Visual Basic logic for metering and dispatching
- Integrated MIL-STD logic into civilian infrastructure
- Developed audit-ready documentation pipelines

Conclusion

The S.E.E.I.S.U.A framework offers a scalable, peace-driven solution to unify energy regulation, industrial metering, and strategic infrastructure across South Union Africa. It empowers municipalities, commissioners, and engineers to collaborate under a shared vision of efficiency, security, and compliance.

Bibliographic References

- MIL-STD-1394: Calibration and metering standards
- IEEE 1459: Power definitions for electrical systems
- SAQA/NQF regulatory frameworks
- City Power Johannesburg technical bulletins
- Tshingombe Fiston internal research archives (2023–2025)

Operational Standards: GENIAC & GENIE CORP MILITAIRE

- GENIAC: Logic-based control systems for metering and dispatch
- GENIE CORP: Military-grade electrotechnical protocols
- MIL-STD Integration:
 - MIL-STD-810 (Environmental Engineering)
 - MIL-STD-461 (Electromagnetic Compatibility)
 - MIL-STD-882 (System Safety)

Would you like this scaffold formatted into a printable Word or LaTeX layout with embedded branding zones, dropdowns for commissioner roles, and reissue logic for regulatory updates? I can also help you build a Visual Basic certificate engine to automate compliance and metering indexing.

OPERATION GENIAC AND GENIE

regulatory depth, and intergovernmental scope. This format is ready for presentation to councils, commissioners, or international partners.

Strategic Report: Support for Energy-Efficient Electrical & Industrial Systems in South Union Africa (S.E.E.E.I.S.U.A)

1. 🔍 Overview

This report outlines a multi-sectoral proposal to establish a unified, energy-efficient electrical and industrial ecosystem across South Union Africa. It addresses regulatory harmonization, infrastructure modernization, and conflict resolution mechanisms between municipalities, city power authorities, and intergovernmental bodies.

2. Background

South Union Africa faces fragmented energy governance, inconsistent metering standards, and unresolved industrial supply conflicts. The S.E.E.E.I.S.U.A initiative proposes a conventional intergovernmental framework to:

- Dispatch and interconnect electrical production.
- Harmonize city power regulations.
- Resolve urban energy conflicts.
- Align industrial trade and compliance across national and international boundaries.

3. ▲ Issue Statement

Current challenges include:

- Load shedding mismanagement.
- Conflicting metering and billing systems.
- Regulatory gaps between city power stations and substations.
- Disputes over industrial supply, job tendering, and energy policy.
- Lack of unified compliance across municipalities and international commissions.

4. ▴ Scope

The initiative spans:

- Peace and eco-system regulation across African energy sectors.
- Harmonization of city power, industrial trade, and material compliance.
- Integration of megawatt financial planning, human resource development, and job regulation.
- Conflict resolution between consumers, suppliers, and power stations.
- Research and doctoral-level design for city power modernization.

5. ■ Description

S.E.E.E.I.S.U.A will:

- Establish a commissioner-led regulatory council.
- Normalize substation and power plant operations.
- Implement metering and cabling standards.
- Oversee demolition and rebuilding of outdated infrastructure.
- Introduce high/low voltage installation protocols.

- Manage tendered job supply chains and remanufacturing systems.

6. Data Inventory & Analysis

Metric	Value/Estimate
Daily kWh per cell	10
Monthly kWh per cell	300
Annual Index (360 days)	3600 kWh
Conflict Load (Imaginary)	70,000 MW
Budget Forecast	50,000 MW / R50 billion
Metering Indicators	Index, %Reg, Voltage

Analysis reveals:

- High variance in city power allowances.
- Discrepancies in consumer vs. plant metering.
- Financial inefficiencies in tendered supply chains.
- Need for forensic audit and intelligence-led regulation.

7. Advantages

- Unified energy governance across regions.
- Reduced conflict between consumers and suppliers.
- Improved job performance and career regulation.
- Enhanced fiscal transparency and tax incentive alignment.
- Integration of atomic safety and regeneration systems.

8. Disadvantages

- High initial cost of infrastructure overhaul.
- Resistance from legacy municipal systems.
- Complexity in harmonizing international regulation.
- Risk of politicization in commissioner appointments.

9. Mission

To promote peace, security, and sustainable energy regulation across South Union Africa through:

- Atomic safety protocols.
- Career regeneration in engineering and energy systems.
- Interregional retransmission and conformance.

10. Vision

A mediation and arbitration commission that:

- Oversees interregional energy policy.
- Manages megawatt financial operations.
- Supports low-consumption treatments and job career pathways.

11. Goal

To establish a semester-based performance cycle for:

- Career development.
- Energy recycling.
- Industrial regeneration.

12. Operational Framework

- Council of Union Trade & Engineering.
- Union Bank for African Energy.
- Industrial conformance rules and job governance.

13. **Module: Infrastructure Overhaul**

- Substation demolition and rebuilding.
- Metering and cabling normalization.
- Motor electrogene system deployment.
- Disarmament of obsolete industrial systems.
- Installation of high/low voltage metering.

14. Regulation Framework

- Power factor demand systems.
- Electrotechnical compliance.
- Industrial electronic manufacturing.
- Conflict resolution in energy media (radio, TV).

- Financial megawatt regulation and audit trails.

Would you like this formatted into a printable Word layout with embedded branding zones, dropdowns for commissioner roles, and reissue logic for regulatory updates? I can also scaffold a Visual Basic certificate engine to automate metering compliance and audit indexing.

DESCRIPTION

This section outlines the operational logic and regulatory integration of GENIAC and GENIE-based systems within the energy, industrial, and security sectors. These modules support intelligent control, safety enforcement, and compliance tracking across urban and intergovernmental environments.

- **GENIAC:** Logic-based control system for metering, dispatching, and infrastructure automation.
- **GENIE SECURITY:** Embedded protocols for infrastructure protection, access control, and cyber resilience.
- **GENIE POLICE:** Regulatory enforcement logic for municipal and industrial energy compliance.
- **GENIE SAFETY:** Safety assurance framework for electrical installations, public infrastructure, and industrial zones.

ANALYSIS

Module	Functionality	Sector Impact
GENIAC	Logic sequencing, control automation	Metering, dispatch, diagnostics
GENIE SECURITY	Intrusion detection, access control	Substations, control rooms
GENIE POLICE	Regulation enforcement, audit logic	City power, industrial zones
GENIE SAFETY	Fault detection, hazard mitigation	Public safety, compliance

- GENIAC enables programmable logic for energy dispatch and metering normalization.
- GENIE SECURITY integrates biometric and digital safeguards for critical infrastructure.
- GENIE POLICE enforces regulatory thresholds, load limits, and compliance audits.
- GENIE SAFETY ensures MIL-STD-grade protection against electrical faults and environmental hazards.

RESEARCH METHOD

The methodology combines:

- **Field audits** of substations, metering installations, and control panels.
- **Simulation modeling** using GENIAC logic blocks for dispatch and load balancing.
- **Security penetration testing** under GENIE SECURITY protocols.
- **Regulatory mapping** aligned with GENIE POLICE enforcement logic.
- **Safety validation** using GENIE SAFETY MIL-STD compliance checklists.

Tools include:

- Visual Basic logic engines
- Embedded microcontroller testbeds
- MIL-STD-882 and MIL-STD-810 compliance matrices
- Environmental hazard simulation platforms

REGULATION SECTOR: ENVIRONMENT

This sector governs the intersection of energy infrastructure and environmental safety, ensuring:

- Compliance with national and international energy safety laws
- Integration of GENIE SAFETY into urban planning and industrial zones
- Monitoring of emissions, thermal discharge, and electrical waste
- Remanufacture and recycling protocols for obsolete infrastructure
- Conflict resolution between consumer demand and environmental limits

Would you like this section formatted into a printable layout with dropdowns for GENIE module selection, MIL-STD compliance zones, and audit trail fields? I can also scaffold a Visual Basic interface to automate GENIE module logging and environmental regulation tracking.

PSIRA
GRADE A, B, C, D, E
CERTIFICATE

SECURITY NAME

TSHINGOMBE
TSHITADI

12 February 2024





**SASSETA Moderator
Assessor
Engineering**

**tshingombe
St Peace College
DHET**

Career Discovery Award Mountaineer

Progress 5 of 12.

★ Expeditioner

You have 21,800 points Earn 13,400 more points to reach Expeditioner rank.

Your Personal

[Your Monthly Learner Report](#)

Become an Agentblazer
Start your Agentblazer journey now with the level!

Amp: Trending
Set your Agentblazer goal, learn

Tshingombe

Engineering Electrical
Johanneburg Gauteng
Teaching Assistant

Engineering
Electrical Engineer

In Progress

- Quick Start: Lightning Web Components
- MuleSoft RPA Design Documentation 55% points

In Progress

- Diploma in Applied Psychology
- Advanced Diploma in High School Chemistry

Completed 0 courses online - 0 closer

Quick Start: Lightning Web Components

Fast track 68%

MuleSoft EPA Design Documentation

Progress 33%

Insurance Quoting Foundations

Fast track 16%

In Progress

★ BuiltWithAgentforce Quest 85%

Quick Start: Build Service Agent with Agentforce

Fast track 85%

Become an Agentblazer Start

your Agentblazer journey now with Agentblazer Champion hall!

[Close](#)

Trending Topics

- Engain Bots
- Digital Engagement
- Tips And Tricks

Trending Topics

Download the New Tshingombe GO!

Courses in November 2025

Learn completed

Goals & Achievements

In job completed

Trending Topics

Trending Topics £83

5-yearly hopes
Researching the market

Downloaded no more
Virtual site

Tshingombe: Your Monthly Learner Report is in!

0 closer 0 dai account no courses to sample
[Learn more](#)

- Diploma in Applied Psychology
- Advanced Diploma in High School Chemistry

tshingombe: Your Monthly Learner Report is in!

7 courses completed MO earned 2 7 days this month

> Or Saco if it's the first month

- 1. ellory 1 day
- 1. shaw Silver 1 day
- 1. Bronze 1 day
- 1. Bronze show 1 day

Goals and Achievements in November

- Completed Courses More fast track
- I completed 0 courses
- Courses completed 0 courses
- 0 courses 5 fees
- 1. rnp. -

Keep learning and more results?

November 2025

Mon	Tue	Wed	Thurs	Fri	Sat
			1	3	3
4	5	6	7	8	9
10	11	12	13	14	15
16	17	18	19	20	21

ons:

J

ig

ve
rch
ices

-
arch
es

er -

ions



PSIRA
Private Security Industry
Regulatory Authority

sasseta

ASSESSOR AND MODERATOR CERTIFICATE

This is to certify that

Tshingombe Tshitadi

at St Peace College

ID Number: TIRCG00091061010

**ASSESSOR AND MODERATOR
CERTIFICATE**

Closing

- Supply
Product
2 Dec 2
- Volunt
Senior
14 Jan
- Transf
31 Dec
- Infrast
Engine
31 Dec
- Comm
Superv
9 Dec 2
- RaSP S
Operat
(SC) EXT



PSIRA

PRIVATE SECURITY INDUSTRY
REGULATORY AUTHORITY

**SASSETA ASSESSOR
MODERATOR
CERTIFICATE**

Awarded to

Tshingombe Tshitadi

at St Peace College

ID Number: TIRCG00091061010

PRIVATE SECURITY INDUSTRY
REGULATORY AUTHORITY

METROPOLITAN

POLICE SERVICE

Certificate Transcript Record | IP LICENSE CAREER PORTAL

Applications

LFR Engineering Supervisor	Review Status	View Application
Infrastructure/DevOps Engineer	View Application	View Application
Leading Engineer - Specialist Search	View Adiration	View Application
Technical Services	Review Status	View Application

The Certificate Record

Learner:

Tshingombe Tshitadi

PSIRA SASSETA Assessor Moderator | Private Security Industry
Safety Engineering | LMS

Certificate Name: **tshingombe Tshitadi**
at St Peace College

POLICE SERVICE



Metropolitan Police Service

CERTIFICATE TRANSCRIPT RECORD

Learner: Name

Tshingombe Tshithitadi

Private Security Industrial PIRIIA
SASSETA Assessor Moderator,
Safety Engineering, LMS

Certificate Name: Tshingombe Tshitadi
at St Peace College

Applications:

Applications

Review Status

View Communications

View Application

View

Applications

LFR Engineering Supervisor

Review Status

Infrastructure/DevOps Engineer

View
Communications

Leading Engineer - Specialist
Search Technical Services

View
Communications



BlockMark REGISTER

CERTIFICATE TRANSCRIPT RECORD

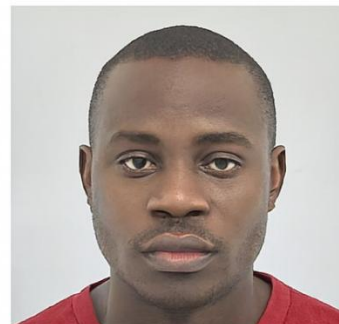
Learner: Name

Tshingombe Tshititadi

(DjoFis)

Private Security Industrial PIIIIA
SASSETA Assessor Moderator,
Safety Engineering, LMS

Certificate Name: Tshingombe Tshititadi
at St Peace College



**Tshingombe Tshithitadi
Fiston**

(DjoFis)

BlockMark ID: 1f227088-3b1b409c-
88c9-87fa715ff7b4

Personal account with certificates

Viewable certificates awarded to this person:



tshingombe tshitadi fiston

(djofis)



info

tshingombe tshitadi fiston's profile picture

BlockMark ID: 1f227088-3b1b-4093-88c9-97fa715ff7b4

Personal account with certificates

Metropolitan Police Service certificate transcript record
ip license career portal

Applications: Made

LFR Engineering Supervisor	Review Status	View Application
Infrastructure/DevOps Engineer	View Application	View Application
Leading Engineer - Specialist Search	Review Status	View Application
Technical Services	Review Status	View Application

the certificate record

learner: name **tshingombe tshitadi**

private security industrial PSIRA SASSETA assess moderator,
safety engineering | LMS

Certificate name: **tshingombe tshitadi** at St Peace
College



Tshigombe Tshitadi Fiston (Djfis)

BlockMark ID:

1f2270888-3blb-409r-38c-99cf 
97ta715ff7fFi4

MODERATOR

ASSESSOR

CAREER

MET METRCPOLITAN



Good morning, tshingombe!

Mountaineer

Progress: 5 of 12.



Vieweable

Expeditioner

You have 21,600 points

Earn 13,400 more points
to reach Expeditioner rank.

LMS St Peace College Academic

Transcript Record



BlockMark ID Transcript Record

Transcript record

Moderator

Assessor



**Tshingombe
Tshitadi Fiston
(Djofis)**

BlockMark ID:
1f227088-3bib-4093-
88c9-97f.a715fffb4

Personal account
with certificates

traihed

Good morning,
tshingombe!



**Mountaineer Progress: 5 of 12
Expeditioner**

You have 21,600 points
Earn 13,400 more points to reach
Expeditioner rank.



LMS ST Peace College Academic

46307064

tshingomberfiston@gmail.com

**Badges
948**

**Trophies
216**

**Reputation
points
0**

**Following
0**



t user

S

image

ngombe

tadi fiston



Tshingombe tshitadi Fiston

(djofis)

BlockMark ID: 1f227088-3b1b-4093-88ce97fa715

Personal account with certificates

Viewable certificates awarded to this person:

- [Metropolitan Police Service certificate](#)
- [Transcript](#)
- [Record IP License](#)
- [Career portal](#)

Applications:

LFR Engineerring Supervisor	Review Status
Infrastructure/DevOps	View Comunications
Engineer	View Application
Leading Engineer - Specialist	View Application
Search Technical Services	Job Advert

LEARNER

tshingombe tshitadi

SASSETA ASSESSMENT
POLICE

at St Peace College

CERTIFICATE

at St Peace College



Microsoft Company

REGISTRATION

This is to certify that

Tshingombe Tshitadi

Product Issue:

HARDWARE • SOFTWARE • NETWORK



Microsoft

LICENSE CERTIFICATE

OF AWARD ENGINEERING

Tshingombe Tshitadi

Product Issue:

HARDWARE • SOFTWARE • NETWORK



GitHub



Azure

Career Portal • St Peace College

Life Is On

Schneider
Electric

LICENSE CERTIFICATE OF AWARD ENGINEERING

Tshingombe Tshitadi

Product Issue:

HARDWARE • SOFTWARE • NETWORK



GitHub



Azure

Schneider
Electric

Electric®

LICENSE CERTIFICATE

OF AWARD ENGINEERING

Tshingombe Tshitadi

HARDWARE • SOFTWARE ENGINEERING
ELECTRICAL

Career Portal • St Peace College

Certificate of Project

AWARDED TO

Tshingombe Tshitadi

For: Issue Term – Private and Public Regulator Policy

Domain: Safety & Security

This certificate attests that the bearer is responsible for the project and commitments in private and public regulation, safety, and compliance.

ISSUE DATE: 04/12/2025

Regulatory Authority

Project: Issue Term – Private & Public
Regulator Policy – Safety and Compliance

Deconstructing Reliability: Inside MIL-STD-11991B Parts, Materials, and Processes (PM&P)

This standard establishes rigorous requirements for every component in a military system, focusing on counterfeit prevention, lifecycle management, and documented quality.

Excerpt from
Appendix H

Key Definitions

Term	Definition
Approved Supplier	Formally assessed supplier with adequate procedures for providing parts/materials, including counterfeit avoidance...
Authorized Supplier	Supplier authorized by the original component manufacturer (OCM) to buy parts directly.
Broker	Unauthorized supplier, typically independent distributor, buying/selling parts without stock or OCM authorization.
COTS item	Commercially Available Off-the-Shelf item: sold in substantial quantities in marketplace and avoidances to authorize inerse physical equiment...
Counterfeit Part	Unlawful/unauthorized reproduction, substitution, or alteration misrepresented as authentic.
Derating	Using components below maximum ratings to improve reliability.

Incoming Inspection Data Requirements (Appendix H)

Requirement	Applies to: EEE parts	Applies to: Mechanical parts	Applies to: Materials
Database fields maintained for life	✓	✓	✓
Documented procedures for tests	✓	✓	✓
Radiological inspection (X-ray)	Yes (as applicable)	✓	—
DPA (Destructive Physical Analysis)	Categories A-B required	—	—
XRF (material discrepancies)	✓	—	—
PIND (Particle Impact Noise Detection)	Categories A-C, T	—	—

PROJECT: N-DIPLOMA FRAMEWORK // DRAWING NO: ELEC-ENG-005

NotebookLM

Building Fluency Across Ecosystems: Integrating Military, Safety, and Commercial Standards

Mastery requires navigating the intersection of military documentation standards (MIL-STD-100G) and international hazard-based safety standards (IEC 62368-1). Understanding both is critical for designing ruggedized, safety-critical systems.

MIL-STD-100G vs. IEC 62368-1:2024

Dimension	MIL-STD-100G	IEC 62368-1:2024
Safety Focus	Critical Safety Items (CSI) & Characteristics	Hazard-Based Safety Engineering (HBSE)
Drawing Practices	Prescriptive drawing formats (ASME Y14.100M)	Performance-based; documentation must support risk assessment
Change Control	Formal revision blocks and engineering evaluation for changes to CSIs	Changes affecting safeguards require an updated risk assessment
Qualification	Source control qualification by design activity	Certification by accredited labs (e.g., CB Scheme, NRTL)

Key Intersection Point:
Risk-Based vs. Prescriptive

Key Intersection Point:
Risk-Based vs. Prescriptive

Pillar 2: The Systemic Navigation Toolkit

Resilience requires a specific skillset for engaging with administrative and legal systems. This involves leveraging official processes, maintaining meticulous records, and understanding the language of regulatory bodies.



Formalizing Disputes

Utilize official channels like the CCMA for dispute resolution to create a formal, documented record of engagement.



Managing Record Integrity

Track all submissions to bodies like DHET and SAQA, documenting dates, names, and statuses to counter delays and build a case for escalation.



Leveraging Regulatory Bodies

File formal complaints with oversight authorities like PSIRA to ensure accountability and trigger official investigation processes.



Engaging Law Enforcement

Use official SAPS processes for documentation, such as point-out notes and case numbers, to create an undeniable record when necessary.

PROJECT: N-DIPLOMA FRAMEWORK // DRAWING NO: ELEC-ENG-012

NotebookLM

Navigating the Labyrinth: The Reality of the Qualification System

“A system plagued by decades-long certification backlogs and administrative irregularities.”

“The lived experience: Unfair dismissal disputes (CCMA), invalidated results, and paused diploma issuance.”

“The core conflict: How does one prove mastery when the system of verification is itself broken?”



NotebookLM

Precision in Practice: The Anatomy of a Military Standard

Compliance is not a high-level concept; it is a granular, data-driven discipline. Mastery requires understanding specific derating factors, material properties, and inspection protocols that guarantee performance under stress.

Table AVI. Microcircuit Derating Factors

Critical Stress Parameter	Digital	Linear
Max Supply Voltage	0.90	0.80
Power Dissipation	0.80	0.75
Max Junction Temperature	-40°C	-40°C

Table AI. Capacitor Derating Factors

Type	Voltage Derating Factor
Ceramic	0.50
Tantalum, Solid	0.50
Plastic Film	0.50
Aluminum Electrolytic	Not allowed

Table XXXI. Fungi Susceptibility of Materials

Group I – Fungus-inert materials	Group II – Fungus-nutrient materials
Acrylics	Epoxy resin
Glass	Rubbers (natural/synthetic)
Metals	Polyvinyl chloride (PVC)
Polyamide	Cellulose acetate
Silicone resin	Lubricants

NotebookLM

Bridging Universes: Integrating Military and Commercial Standards

True expertise lies in synthesizing requirements across different regulatory domains. By integrating the rigorous documentation of MIL-STD-100G with the hazard-based safety engineering of IEC 62368-1, a comprehensive framework for designing ruggedized, safe, and globally compliant products emerges.

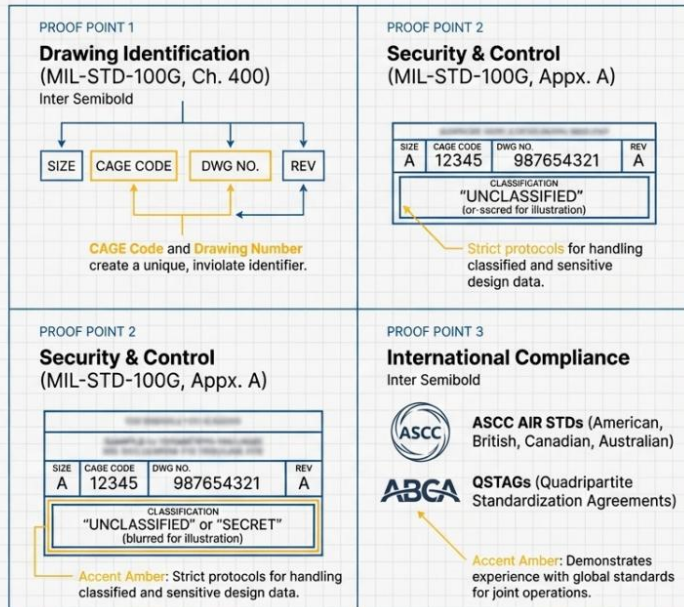
Dimension	 MIL-STD-100G (Engineering Drawings)	 IEC 62368-1:2024 (Safety Standard)
Safety Focus	Critical Safety Items (CSI) identified on drawings.	Hazard-Based Safety Engineering (HBSE).
Documentation	Prescriptive drawing formats (ASME Y14.100M).	Documentation of hazards, safeguards, and risk assessments.
Change Control	Formal revision blocks and Configuration Management.	Changes affecting safeguards require updated risk assessment.
Qualification	Source control drawings for government approval.	Testing and certification by accredited labs (e.g., CB Scheme).

NotebookLM

Pillar I: Grounded in Foundational Engineering Standards

Inter Regular

Mastery of engineering drawing standards (MIL-STD-100G) ensures absolute clarity, interoperability, and configuration management in complex defense and aerospace systems.



NotebookLM

Managing the Lifecycle: Parts, Materials, and Processes

A disciplined approach to Parts, Materials, and Processes (PM&P) management, aligned with MIL-STD-11991B, is critical for ensuring reliability, preventing component failure, and mitigating supply chain risks like counterfeit parts.



NotebookLM

Case Study: Digital Certificates & Immutable Audit Trails

Using platforms like **BlockMark**, the framework provides **verifiable, time-stamped** proof of certifications and inspections, crucial for high-stakes environments like public sector tendering.

Inspection Time:
Thursday 6th March 2025 - 08:49:36(GMT)

BlockMark Registry

A certificate inspection by tshingombe tshitadi fiston

tshingombe tshitadi fiston inspected SAFETY SHIELD GLOBAL LIMITED's Cyber Essentials certificate on Thursday 6th March 2025 - 08:49:36(GMT)

Field Name	Value when inspected	Current Value	Same Value
Certificate ID	CE-12345678	CE-12345678	Yes ✓
Organization	SAFETY SHIELD GLOBAL LIMITED	SAFETY SHIELD GLOBAL LIMITED	Yes ✓
Certification Scheme	Cyber Essentials	Cyber Essentials	Yes ✓
Issue Date	2024-01-15	2024-01-15	Yes ✓
Expiry Date	2025-01-15	2025-01-15	Yes ✓
Certification Body	IASME Consortium	IASME Consortium	Yes ✓
Inspector ID	T-FISTON-001	T-FISTON-001	Yes ✓
Inspection Status	Valid	Valid	Yes ✓

Audit Trail: Compares 'Value when inspected' vs 'Current Value' to verify integrity.

Application: Validating supplier credentials for tenders (Eskom, City Power) and ensuring ongoing compliance.

